UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,224	01/16/2002	Mototsugu Nishioka	500.41092X00	4402

86636 7590 01/12/2010

BRUNDIDGE & STANGER, P.C.
1700 DIAGONAL ROAD, SUITE 330
ALEXANDRIA, VA 22314

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
01/12/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MOTOTSUGU NISHIOKA, HISAYOSHI SATOH, and YOICHI SETO

Appeal 2009-001507
Application 10/046,224[1]
Technology Center 2400

Decided: January 12, 2010

Before LEE E. BARRETT, HOWARD B. BLANKENSHIP and JAY P. LUCAS, *Administrative Patent Judges*.

LUCAS, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] Application filed January 16, 2002. Appellants claim the benefit under 35 U.S.C. § 119 of Japan application 2001-009,646 filed January 18, 2001. The real party in interest is Hitachi, Ltd.

STATEMENT OF THE CASE

Appellants appeal from a final rejection of claims 23-44 under authority of 35 U.S.C. § 134(a). The Board of Patent Appeals and Interferences (BPAI) has jurisdiction under 35 U.S.C. § 6(b).

We affirm the rejections.

Appellants' invention relates to a public key cryptographic method for private communication with high security. In the words of Appellants:

> In order to achieve the above objects of the invention, a ciphertext is created by using a combination of a plaintext and random numbers in order to reject an illegal ciphertext input to a (simulated) deciphering oracle and to guarantee security against adaptive chosen ciphertext attacks. The environment given a deciphering oracle means an environment which unconditionally gives the deciphered results of any ciphertext excepting a target ciphertext. According to one of specific public-key cryptographic schemes, the following secret-key is created:
>
> - $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$
>
> and the following public key is created:
>
> - p, q : prime number (q is a prime factor of p-1)
> - $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
> - $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p$, $d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p$, $h = g_1^{z} \bmod p$,
> - k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$

(Spec. 5, l. 15 to 6, l. 5).

Claim 23 is exemplary:

23. A public-key cryptographic method implemented in a computer system comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $\quad G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d_1 = g_1^{y_{11}} g_2^{y_{12}}$, $d_2 = g_1^{y_{21}} g_2^{y_{22}}$, $h = g_1^{z}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 \| \alpha_2 < q \qquad (\forall \alpha_1 \in X_1,\ \forall \alpha_2 \in X_2)$$

where M is a plaintext space;

a ciphertext generation and transmission step of selecting random numbers $a_1 \varepsilon X1$, $a_2 \varepsilon X_2$, $r \varepsilon Zq$ for a plaintext m ($m \varepsilon M$), calculating:

$$u_1 = g_1^{r}, \quad u_2 = g_2^{r}, \quad e = \pi(\alpha_1, \alpha_2, m) h^{r}, \quad v = g_1^{\alpha_1} c^{r} d_1^{\alpha r} d_2^{mr}$$

where $a = a_1 \| a_2$, and, and transmitting (u_1, u_2, e, v) as a ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by

using the secret key, a'_1, a'_2, m' ($a'_1 \varepsilon X_1$, $a'_2 \varepsilon X_2$, $m' \varepsilon M$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = e/u_1{}^{x}$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+m' y_{21}} u_2{}^{x_2+\alpha' y_{12}+m' y_{22}} = v$$

outputting m' as the deciphered results (where a' = $a'_1 \| a'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Cramer	US 6,697,488 B1	Feb. 24, 2004

REJECTIONS

The Examiner rejects the claims as follows:

R1: Claims 23, 28, 35 and 40 stand rejected under 35 U.S.C. § 112, second paragraph, for being indefinite, for failing to particularly point out and distinctly claim the subject matter which Appellants regard as their invention.

R2: Claims 24, 40, and 41 stand rejected under 35 U.S.C. § 112, second paragraph, for being indefinite (as above).

R3: Claim 30 stands rejected under 35 U.S.C. § 112, second paragraph, for being indefinite (as above).

R4: Claim 36 stands rejected under 35 U.S.C. § 112, second paragraph, for being indefinite (as above).

R5: Claims 28, 40, and 41 stand rejected under 35 U.S.C. § 112, second paragraph, for being indefinite (as above).

R6: Claims 23-44 stand rejected under 35 U.S.C. § 103(a) for being obvious over Cramer.

Groups of Claims:

The claims will be addressed in the order of the rejections, grouped in accordance with the arguments.

Appellants contend that the claims are definite and that the claimed subject matter is not rendered obvious by Cramer. The Examiner contends that each of the three groups of claims is properly rejected.

Only those arguments actually made by Appellants have been considered in this opinion. Arguments that Appellants could have made but chose not to make in the Briefs have not been considered and are deemed to be waived.

ISSUE

The issue with regard to the rejection under 35 U.S.C. § 112 is whether Appellants have shown that the Examiner erred in rejecting the claims for being expressed in an indefinite manner. The issue with regard to the rejection under 35 U.S.C. § 103 is whether Appellants have shown that the Examiner erred in concluding the claims to be obvious over Cramer. The second issue turns on whether the specific elements in Appellants' equations describing the nature of their public and private key, and in the equations describing the ciphertext generation are obvious over the somewhat different equations taught in the Cramer reference.

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence.

1. Appellants have invented an improved public key cryptographic method for generating the ciphertext of a plaintext message (Spec 5, l. 8). The method is resistant to attacks using the adaptive chosen ciphertext code breaking technique as it rejects illegal ciphertexts (Spec. 5, l. 20). The method develops a seven element secret-key described as:

   > x_1, x_2, y_{11}, y_{12}, y_{21},y_{22}, z included in the set Z_q

   The method also develops a public key involving the variables g_1, g_2, c, d, and h and satisfying a number of conditions including a $d_1=g_1^{y11}g_2^{y12}$, and a $d_2=g_1^{y21}g_2^{y22}$.

2. The Cramer reference is addressed to a public key cryptosystem that generates pubic and private keys for encrypting messages (Col. 4, l. 19). The Cramer teachings provide a public key cryptosystem that is secure against an adaptive chosen ciphertext attack by rejecting illegitimate ciphertexts (Col. 9, l. 17; col. 4, l. 12). The method teaches choosing a private key described as :

   > x_1, x_2, y_1, y_2, z included in the set Z_q

   The Cramer method also develops a public key using formulas to develop the values g_1, g_2, c, d, and h.

3. The field of formulating the mathematics for the generation of cryptosystems is a highly advanced field of extreme complexity and

competitive challenges for both protecting data and for breaking the protection (Spec. 1 – 3; Cramer col. 1, ll. 19 to col. 2, ll.35).

PRINCIPLES OF LAW

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of prima facie obviousness or by rebutting the prima facie case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

"Indefiniteness under 35 U.S.C. § 112 ¶ 2 is an issue of claim construction and a question of law that we review de novo." *Cordis Corp. v. Boston Scientific Corp.*, 561 F.3d 1319, 1331 (Fed. Cir. 2009) (citing *Praxair, Inc. v. ATMI, Inc.*, 543 F.3d 1306, 1319 (Fed. Cir. 2008)).

Appellant may sustain its burden by showing that where the Examiner relies on a combination of disclosures, the Examiner failed to provide sufficient evidence to show that one having ordinary skill in the art would have done what Appellant did. *United States v. Adams*, 383 U.S. 39 (1966); *In re Kahn*, 441 F.3d 977, 987-988 (Fed. Cir. 2006); *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick, Co.*, 464 F.3d 1356, 1360-1361 (Fed. Cir. 2006). The mere fact that all the claimed elements or steps appear in the prior art is not *per se* sufficient to establish that it would have been obvious to combine those elements. *United States v. Adams*, *supra*;

Smith Industries Medical systems, Inc. v. Vital Signs, Inc., 183 F.3d 1347, 1356 (Fed. Cir. 1999).

"[T]he words of a claim 'are generally given their ordinary and customary meaning.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (internal citations omitted). "[T]he ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Id.* at 1313.

ANALYSIS

From our review of the administrative record, we find that the Examiner has explained the rejections of Appellants' claims under 35 U.S.C. §§ 112 and 103 on pages 4 to 23 of the Examiner's Answer. In opposition, Appellants present a number of arguments.

Arguments with respect to the rejection
of claims 23, 28, 35 and 40 [R1]
claims 24, 40 and 41 [R2]
claim 30 [R3]
claim 36[R4] and
claims 28, 40 and 41[R5]
under 35 U.S.C. § 112 paragraph 2

The Examiner has rejected each of the noted claims for being indefinite, in the sense that the recited values (e.g., a_1, a_2, q, G, g_1, g_2 etc.) are expressed in the claims as mere variables, letters and numbers, with no definition of "how those elements are generated or obtained and/or what they are intended to be, thus the metes and bounds of the claims are not definite." (Ans. 24, middle).

Appellants have responded in the Brief with a mere assertion that the claims are definite (App. Br. 16, middle). In the Reply, Appellants state that an antecedent basis is provided for the terms in the sense that the same term is referred to as "the ciphertext" when "ciphertext" has been referred to previously in the claims (Reply Br., 4-9). Appellants' response does not address the point made by the Examiner.

This is an art of very high complexity (FF #3), and the practitioner in such an art is assumed to have advanced math skills. But the attachment of meaning to the variables expressed in the equations of the claims, either through definitions in the specification or in the claims themselves, adds necessary clarity to the claims to be able to properly appreciate the metes and bounds of the protected invention. Appellants have not done this. The Examiner's contrast of the instant claims to those in the prior art was insightful (Ans. 25, top). We find that Appellants' bare assertion of compliance with 35 U.S.C. § 112, paragraph 2, and discussion of antecedents of expressions in the formulae did not persuasively counter the Examiner's rejection.

We thus find that Appellants have not established error in the rejections [R1] to [R5] of the noted claims under 35 U.S.C. § 112, paragraph 2.

Arguments with respect to the rejection of claims 23 to 44 under 35 U.S.C. § 103(a)[R6]

The Examiner has rejected claims 23-44 for being obvious over Cramer. Cramer presents a system and method for encrypting plaintext to

ciphertext and decrypting back to the plaintext using the same five stages expressed in the claims (Col. 6, ll. 40-65; FF #1, FF#2). Appellants point out certain differences in the formulas used by the reference, and how they are different from the formulas of the claims (App. Br. 17-22, further expanded for each claim in App. Br. 22-55).

Appellants present the same set of arguments against the rejection in the discussion of each of the claims, with minor variations based on the presence or absence of a certain claim limitation. We will thus address the main arguments directly and consider the variations as they arise.

Appellants first argue that certain claims are different from the Cramer reference for their exclusion of the hash function in the formulas (App. Br. 18, top). Appellants point to the use of the hash function H in Cramer's encryption step (Col. 8, l. 10):

$$u_1=g_1^r, u_2=g_2^r, e=h^r m, a=H(u_1,u_2,e), v=c^r d^{ra}.$$

Appellants explain that various cryptographic schemes are based on various assumptions and that some are not always realistic. "The collision intractability of the hash function has not yet been verified (see pages 3, line 27 to page 4, line 24 of the present application)." (App. Br. 18, middle). Thus, Appellants do not rely on the hash function for the encryption step recited in independent claims 23, 24, 28, 30, 40, and 41. In contrast, we note that in the ciphertext generation step of claim 35, Appellants choose to use the hash function:

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad v = g_1^{\alpha_1} c^r d^{\alpha r} \bmod p, \quad K = H(h^r \bmod p)$$

where

- H : hash function

The Examiner points out that "Cramer teaches that the use of a hash function can be omitted (col. 9, lines 60-67)." (Ans. 25, bottom). The discussion in Cramer is in the context of increasing or decreasing the amount of calculation that must be performed to encode the ciphertext and recover the plaintext as a tradeoff against the degree of protection that one desires (*id.*). Mere "lunch-time" attacks, by a casual intruder, can be thwarted by a lesser degree of protection, but serious "adaptive chosen ciphertext attacks" require a higher degree of protection and, the user may be willing to invest the time and effort to perform the increased computations that this higher level requires. (Cramer, col. 2, l. 48). While the mathematics are highly complex in this technical field, we do find that the stated balance of computational difficulty versus higher security is a theme running through both Appellants' disclosure and the Cramer reference. The Examiner indicates that the choice of the presence or absence of the hash function in the equation ciphertext generation would be an obvious variant in view of the teachings of Cramer. We do not find the Appellants to have demonstrated error in that conclusion.

Appellants next argue that "In Cramer, the public key includes one element 'd' as shown in Fig. 2 and as discussed at column 7, lines 26 to 39 thereof. The element 'd' as per Cramer relates to the two elements y_1 and y_2 of the private key." (App. Br. 19, bottom).

Thus in Cramer the public key is defined (partially) as follows:

> Next, a first group-number c, a second group-number h, and a third group-number d are derived in a generation step 15 from the chosen numbers

> g_1, g_2, x_1, x_2, y_1, y_2, z by using calculating means according to the following formulas:
>
> $$c=g_1^{x1}g_2^{x2},\ d=g_1^{y1}g_2^{y2},\ h=g_1^{z}$$
>
> The public key is now complete and is represented by the numbers g_1, g_2, c, d, and h.

(Col. 7, ll. 19-17).

Cramer thus teaches one variable d, relating to y_1 and y_2 (App. Br. 19, bottom). Appellants distinguish their claims 23, 24, 28 and 30 which contain two variables d_1 and d_2.

- $c = g_1^{x_1} g_2^{x_2} \bmod p,\ d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p,\ d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p,\ h = g_1^{z} \bmod p,$

In explaining the advantages of the single variable, d, Appellants contend, "To improve the efficiency of the encryption system, i.e. to reduce the calculation amount of v, it is preferable that the number of d (the value of k) is small." (App. Br. 21, bottom).

In establishing their point, Appellants quote from a treatise by the authors of the Cramer reference. That line of reasoning is as follows:

> At first, (u_1, u_2, e) is replaced with $(a_1,\ldots,a_k)$, where $0 < a_i < q$.
>
> Further, $d_i=(g_1)^{y\_\{i1\}}(g_2)^{y\_\{i2\}} \bmod p$, where $0<i<k$ is calculated and made open.
>
> In the above-mentioned encryption, the calculation of v is replaced with:
>
> $$v=c^r(d_1)^{ra\_1}\ldots(d_k)^{ra\_k}$$

We find, in this equation, that the number of d factors is a discretionary number, depending on the amount of security that the user requires and the amount of computation that the application can withstand.

The Examiner contends that Cramer's patent also suggests a varying number of d variables, depending on the amount of security that the user desires. "Examiner respectfully submits that Cramer teaches "d_i" (Cramer, section V, column 9 [line 58]), thus 'd_i' can change and varies." (Ans. 26, top).

With regard to claim 23, Appellants contend that

> The secret key includes x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, and z. The public key includes elements d_1 and d_2. The element d_1 relates to the elements y_{11} and y_{12} of the secret key, and the element d_2 relates to the elements y_{21} and y_{22} of the secret key. Cramer does not disclose this feature.

(App. Br. 22, bottom)

In summary with respect to this point, the reference Cramer teaches or suggests that the number of "d" variables may be varied in choosing the elements for the private key, with the computations and security changing in a known way depending on the chosen complexity of the key (Cramer, col. 9, l. 58). The Examiner has considered the choice to be obvious to one of ordinary skill in this art, and we do not find that conclusion in error.

In Cramer, the secret key, called the private key, is derived and chosen as follows:

> In the private-key choosing step **13** from a set of elements modulo q, denoted as Z_q and indicated by reference number **14**, for the private key a first exponent-number x_1, a second exponent-number x_2, a third exponent-number z, a fourth exponent-number y_1, and a fifth exponent-number y_2 are chosen at random. This can be expressed as follows.
>
> $$x_1, x_2, y_1, y_2, z \in Z_q$$

(Cramer, col. 7, ll. 15 – 24).

Appellants argue that their invention, as recited in claims 23, 24, 28 and 30, uses four elements of y in the private key, namely:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

(App. Br. 20, middle).

Appellants argue that this difference may appear small, but that it has a large effect (*id.*). The Examiner contends that the differences are within the knowledge of the prior art, as evidenced by Cramer's statements that the d, y_1, y_2 and hash function are typically added to enhance the security of an encryption from the above lunch-time attacks to guard against more determined assaults (Cramer, col. 9, ll. 65-68).

We have considered Appellants' arguments and do not find them compelling of error. The presence of two or four or a variable number of "y" values in this complicated art is suggested by the reference's discussion of the balance of complication of computation versus security of the message, noted above.

Appellants have argued differences from the reference in the calculation of the ciphertext generation and transmission steps (App. Br. 25, top) and the formula for rejecting an improper ciphertext (App. Br. 26, middle). We agree with the Examiner that these expressions have not been

demonstrated to be more than obvious changes to the prior art (Ans. 26, 27). Cramer uses very similar formulae for the encryption, validation, and decryption (Cols. 7 – 9), and we find the differences of the claims from the prior art to be within the scope of the considerable abilities of a skilled person in this art.

As the basic argument of simplicity of calculation versus strength of encryption is repeated with local computational variation in the arguments for each claim, we extend our findings to cover all the claims of the rejection.

CONCLUSIONS OF LAW

Based on the findings of facts and analysis above, we conclude that the Examiner did not err in rejecting claims 23, 24, 28, 35, 36, 40, and 41 under 35 U.S.C. § 112, paragraph two, and did not err in rejecting claims 23-44 under 35 U.S.C. § 103(a).

DECISION

R1: The Examiner's rejection of claims 23, 28, 35, and 40 under 35 U.S.C. § 112, second paragraph, for being indefinite is affirmed.

R2: The Examiner's rejection of claims 24, 40, 41 under 35 U.S.C. § 112, second paragraph, for being indefinite is affirmed.

R3: The Examiner's rejection of claims 30 under 35 U.S.C. § 112, second paragraph, for being indefinite is affirmed.

R4: The Examiner's rejection of claims 36 under 35 U.S.C. § 112, second paragraph, for being indefinite is affirmed.

R5: The Examiner's rejection of claims 28, 40, and 41 under 35 U.S.C. § 112, second paragraph, for being indefinite is affirmed.

R6: The Examiner's rejection of claims 23-44 under 35 U.S.C. § 103(a) for being obvious over Cramer is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

peb

BRUNDIDGE & STANGER, P.C.
1700 DIAGONAL ROAD, SUITE 330
ALEXANDRIA, VA 22314